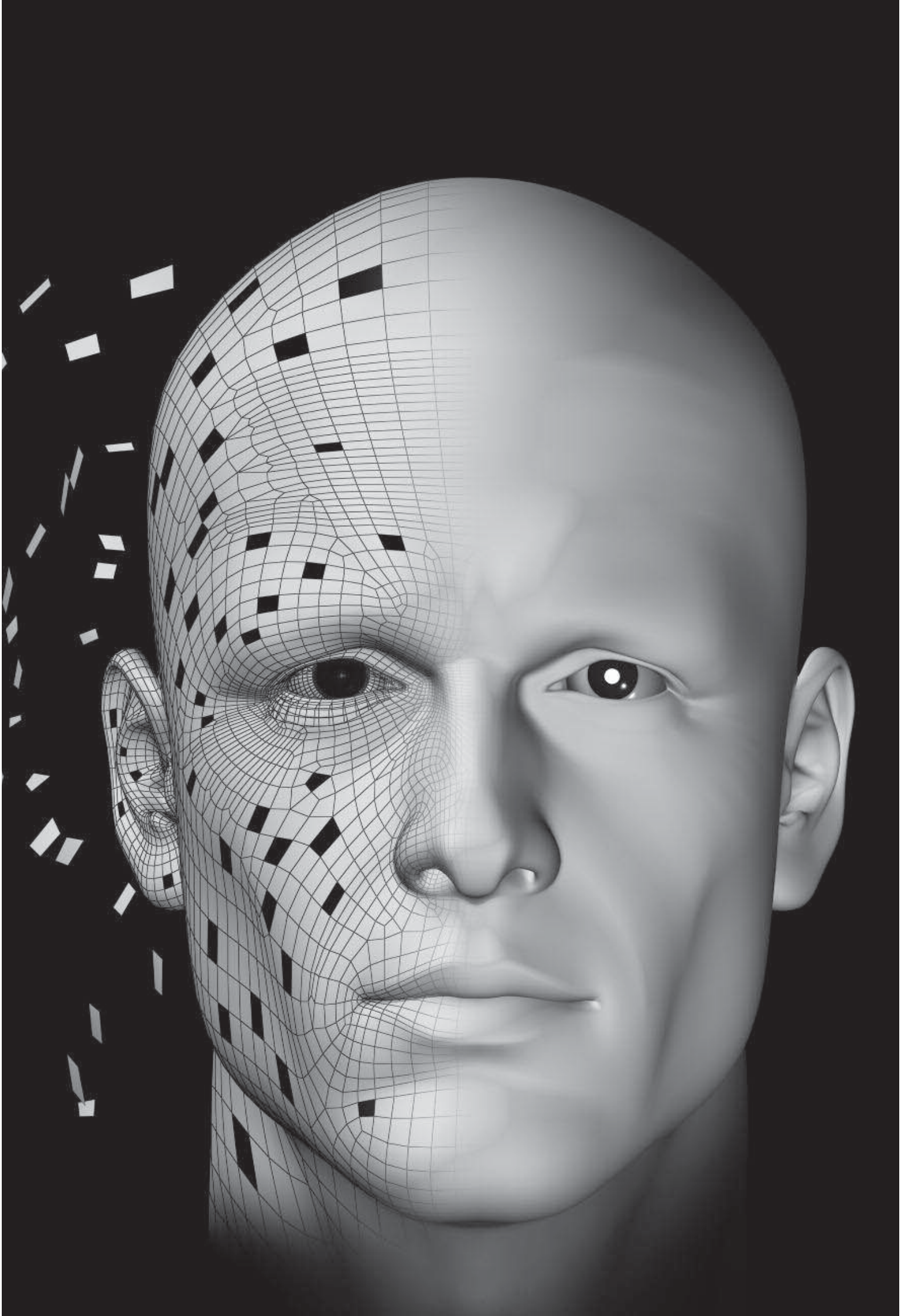

Mª TERESA HEREDERO CAMPO

La memoria de Internet a debate: primeros pasos hacia el reconocimiento del derecho al olvido

El análisis que a continuación se va a realizar del renombrado *derecho al olvido*, pretende acercar al lector uno de los temas de mayor actualidad en la Red, pues en los últimos tiempos ha alcanzado gran relevancia.

Resulta evidente que facilitar datos personales o editar ciertos contenidos en Internet supone, incluso sin que se percate su titular, un riesgo para la intimidad, el honor y la propia imagen. Se trata de datos cedidos que, recopilados por terceros, pueden acabar perjudicando al propio usuario mediante la elaboración de perfiles, compraventa de tales datos, utilización para envíos publicitarios, etc. o cuya simple pervivencia, más allá del control del usuario, puede llegar a afectar a su vida de forma negativa en un futuro más o menos cercano.

Con el uso masivo de las redes sociales la problemática se magnifica considerablemente, y llega aún más allá cuando se trata de menores que sin ningún pudor cuelgan sus fotos más comprometidas en los perfiles que se han creado en cualquiera de las redes sociales hoy existentes, o dan difusión de las mismas a través de cualquiera de las aplicaciones que nos ofrecen hoy las nuevas tecnologías.

A continuación, como punto de inicio, se partirá de la conceptualización del término derecho al olvido, siendo obligatoria la reseña al concepto de *dato de*

Mª Teresa Heredero Campo (email: theredero@usal.es)
Facultad de Derecho. Universidad de Salamanca

Recibido: 14-11-2014. Aceptado: 26-11-2014
Citación: Heredero Campo, Mª Teresa (2014). "La memoria de Internet a debate: primeros pasos hacia el reconocimiento del derecho al olvido". *Tábula,* n. 17, pp. 45-59

carácter personal. En este artículo se analiza la situación actual con respecto al tratamiento de los datos personales, de forma especial en el entorno de las redes sociales, al tiempo que se trata de dar una visión general orientada a la necesidad de la efectiva aplicación de lo contemplado en el *Reglamento de Protección de Datos de la Unión Europea*.

Pese a abordar el tema desde una perspectiva eminentemente práctica, se apuntará la normativa de aplicación y se llevará a cabo una ponderación de los derechos a la intimidad, libertad de expresión y protección de datos.

Análisis de la situación actual: la importancia del reconocimiento efectivo del llamado derecho al olvido

Internet contribuye activa y notoriamente al desarrollo de procesos de información, comunicación, intercambio y generación de nuevos contenidos. En este sentido la *Web 2.0*[2], nos ha aportado grandes avances al colocar al usuario como centro de la información y generador de contenidos.

El riesgo principal que entraña es que el usuario no solo aporta datos de forma consciente, sino que también lo hace de manera inconsciente mientras navega.

Con carácter previo, para entender con mayor claridad el alcance de la cuestión, se hace necesario un acercamiento a dos conceptos que pasamos inmediatamente a analizar: derecho al olvido y dato de carácter personal.

Análisis conceptual de los términos "derecho al olvido" y "dato personal"

El *derecho al olvido*, como tal, no es más que una representación del derecho a la cancelación de los datos cuyo titular no quiere que aparezcan en la Red, o en otras palabras, es el derecho que a través de su legal reconocimiento permite a cualquier individuo cancelar sus antecedentes informáticos (la información que un día quedó recogida y almacenada en la Red y que ahora se pretende suprimir).

El objetivo de su reconocimiento no es otro que tratar de dotar a los individuos de mecanismos reales y efectivos para controlar sus propios datos personales.

Respecto a la definición[3] de *dato de carácter personal*, el propio artículo 3 *de la Ley de Protección de Datos de Carácter Personal (LOPD)*, preceptúa que por tal se entiende "cualquier información concerniente a personas físicas identificadas o identificables".

Dicho término debe considerarse de forma amplia para que pueda adaptarse a la sociedad actual y, por tanto, al uso de las nuevas tecnologías. Con ello se pretende que el concepto alcance incluso a la persona cuyo nombre se desconoce pero cuyo perfil completo se tiene[4], y que por lo tanto puede acabar siendo identificada con toda precisión conforme a dichos datos.

En consecuencia, la Agencia Española de Protección de Datos (AEPD) propone a este respecto que no sea necesario que el dato identifique directamente a la persona sino que sirva para su identificación junto con otros elementos (identificabilidad) a la hora de considerar el concepto de dato personal[5].

Derecho al olvido y redes sociales

Muchas veces, el poder participar de las múltiples herramientas que Internet ofrece, exige el previo registro como usuario de la página a la que se desea acceder bien para consultar una información, participar en un foro, escribir un comentario en un *blog* o acceder a las ofertas laborales que contienen páginas como *Infojobs, Monster, Tutrabajo, Redtrabaja*, entre otras. Este mecanismo no difiere mucho respecto al procedimiento que se ha de seguir cuando lo que se pretende es crear un perfil y poder disfrutar así del mundo de las redes sociales. Se podría decir generalizando, que todas estas aplicaciones tan distintas en sus fines comparten el denominador común de requerir que el usuario se vea obligado a facilitar una serie de datos personales.

Se plantean a partir de este punto varias preguntas: ¿qué ocurre con los datos que se facilitan al registrarse en una página web?, ¿el usuario es capaz de conocer en cuántas páginas está registrado?, ¿se leen las políticas de privacidad de los sitios que se visitan?, ¿son realmente los usuarios conscientes de la cantidad de datos que sobre su vida privada circulan en Internet?

Estas y otras preguntas comienzan a cobrar importancia cuando la sociedad se hace eco de noticias como las publicadas en prensa en los últimos meses, sirva a modo de ejemplo la que ponía de manifiesto que un estudiante de 24 años había sido capaz de forzar a *Facebook* a mejorar la privacidad de sus usuarios. En este caso en concreto el joven logró recuperar 1222 páginas en un CD con datos privados e incluso informaciones y conversaciones que había borrado[6]. Esta y otras muchas noticias en la misma línea, hacen que los usuarios de Internet nos cuestionemos sobre si es obligatorio sentirse perseguido por el pasado, o si somos conscientes de toda la información que facilitamos y en manos de quién está. Otra noticia que saltaba a los medios de comunicación hace algún tiempo decía: "La aplicación para móviles de *Twitter* guarda datos privados de sus usuarios"[7]; entre la información almacenada estaban incluidos nombres completos, correos electrónicos y números de teléfonos de los contactos guardados en la agenda. Los ejemplos son infinitos; una última noticia a destacar, por razones de extensión, ponía en entredicho la seguridad de la aplicación telefónica más popular para enviar mensajes gratuitos de forma instantánea, *WhatsApp*[8]. Esta aplicación cuenta en la actualidad con más de 600 millones de usuarios[9]. El problema radica en que su sistema de cifrado es prácticamente nulo, lo que hace que sea muy fácil acceder a la información de cualquier usuario, aunque se ha venido trabajando mucho en los últimos meses sobre esta cuestión y en el mes de noviembre del presente año

ya salían a la luz noticias que ponían de manifiesto la considerable mejora en el sistema de cifrado y el nivel de seguridad de la aplicación[10]. Además se informa sobre el hecho de que todas las conversaciones quedan almacenadas en una base de datos y no se pueden eliminar pese a que el usuario las borre del registro del teléfono.

La repercusión que noticias como las reseñadas tienen de cara a la sociedad es que provocan un cierto grado de preocupación en los internautas respecto de la seguridad y privacidad de sus datos en Internet, especialmente cuando hablamos de redes sociales (las más comunes *Facebook* y *Tuenti*). Por esta razón no es de extrañar que cada vez sean más los usuarios que limitan el acceso a sus datos solo a personas conocidas, o establecen estrictas restricciones en la configuración de la privacidad de sus perfiles.

Debemos tener en cuenta que una información descontextualizada puede acarrear problemas no solo personales sino sociales y laborales. En la Sociedad de la Información no solo del *currículum vitae* depende el futuro laboral, es igualmente importante lo que Internet pueda decir de una persona. No son pocos los casos vinculados a despidos laborales por contenidos publicados en redes sociales, o empresas que previamente a realizar una entrevista rastrean la información que Internet les pueda proporcionar de los candidatos.

La preocupación de los internautas que pretenden cancelar cierta información sobre sí mismos, no es por lo tanto infundada. Según datos oficiales de la AEPD[11], las reclamaciones recibidas de personas que solicitan que sus datos sean eliminados de la Red de forma permanente se han multiplicado en los últimos años en más del 200% y ello tiene su razón de ser en las innumerables complicaciones que surgen cuando el usuario decide que quiere borrarse de forma total y permanente del *cibermapa*. Porque, aunque no lo creamos, desaparecer de Internet no es tarea fácil. Toda la información que se va facilitando queda grabada en la Red de forma permanente.

Para entender la magnitud del problema se han de tener en cuenta los datos sobre el sorprendente número de usuarios que participan en las redes sociales, así por ejemplo cabe referenciar cómo el crecimiento de registros más significativo ha sido el de *Facebook*, que en el mes de junio de 2014 contaba con más de 1320 millones de usuarios registrados; seguido de otras como *Twitter, Bebo, Myspace o LinkedIn*[12] sin olvidarnos de la española *Tuenti*[13].

El verdadero problema comienza cuando el usuario, consciente de que cierta información no le favorece, quiere borrar algunos contenidos para que desaparezcan de forma permanente[14]; sin embargo, en ocasiones la opción que el usuario encuentra no ofrece garantía alguna de que ese contenido seleccionado vaya a desaparecer sin dejar rastro. Por poner un ejemplo, *Facebook* permite cancelar la cuenta de forma temporal sin mayores impedimentos que hacer *click* sobre el ratón, sin embargo la información continúa activa aunque bloqueada. Si lo

que el usuario solicita es borrarse, los obstáculos son mucho mayores, tal vez son un último intento para disuadir al cibernauta de su voluntad de desaparecer.

Un ejemplo es el reseñado anteriormente en relación con la noticia sobre el estudiante que forzó a *Facebook* a mejorar su seguridad pues, gracias a su perseverancia, consiguió que esta red social se comprometiera a realizar mejoras entre las que se incluyen: dotar de una mayor transparencia a la gestión de las informaciones personales, impedir que cualquier imagen del usuario sea utilizada con fines comerciales sin haber obtenido previamente su consentimiento, eliminar la información que la red social obtiene a través del botón «me gusta», consiguiendo también que se limite el tiempo que *Facebook* puede conservar informaciones sobre la navegación del usuario, como, por ejemplo, las búsquedas que ha hecho y cuándo utiliza otros *plug-ins*[15]. Respecto de esta última cuestión referente al tiempo de conservación de los datos, el Grupo de Trabajo del Artículo 29 (GT29)[16] viene afirmando que los períodos de retención de los datos tienen que ser reducidos al mínimo y ser proporcionales a las finalidades que se persigan[17].

Pero no solo esta nueva tendencia social a procesar la vida privada públicamente va a poner en riesgo algo tan importante como la intimidad. La otra gran amenaza la encontramos en relación con los motores de búsqueda, con respecto a la indexación de contenidos fruto, en gran medida, de las aportaciones realizadas por los propios usuarios en las distintas páginas que conforman la gran biblioteca universal que supone Internet.

En este sentido, y pese a la errónea creencia de que no hay nada que hacer, que no somos dueños de nuestro propio destino digital, o que no podemos decidir sobre los datos que queremos o que no queremos que aparezcan en la Red, la reciente sentencia del Tribunal de Justicia de la Unión Europea (TJUE) de 13 de mayo de 2014 ha logrado arrojar un poco de luz sobre la cuestión debatida, reduciendo la preocupación al determinar la responsabilidad de Google por vulnerar el derecho a la protección de datos[18], reconociendo por primera vez el derecho al olvido con carácter digital. La sentencia reconoce el derecho de los usuarios a solicitar que los motores de búsqueda eliminen determinados resultados de consultas que incluyan su nombre si los derechos de privacidad de la persona prevalecen sobre los intereses en esos resultados[19].

Y es que no se puede pasar por alto que el uso de los motores de búsqueda hace que se pueda encontrar información casi de cualquier cosa o persona. Basta poner en *Google* el nombre y los apellidos de alguien para obtener datos como el domicilio, el teléfono, alguna foto, su *website*, una dirección de correo electrónico, el número de su documento de identidad o información publicada en boletines oficiales por temas como listados de oposiciones, sanciones administrativas o, incluso, temas penales.

En palabras del exdirector de la AEPD, Artemi Rallo[20], en la medida que la actividad de los buscadores se centra principalmente en asociar los términos de

búsqueda a los sitios webs en los que consta esta información, el ejercicio de los derechos de cancelación u oposición debería estar asociado a un ejercicio correlativo de tales derechos frente a los responsables de estos sitios que son quienes permiten el acceso a la información personal[21].

Se puede abrir una nueva brecha de debate, ¿el consentimiento prestado de forma válida previamente puede ser revocado en un momento posterior?, el artículo 14 de la LOPD reconoce el carácter revocable del consentimiento prestado en relación a la comunicación de los datos de carácter personal. Si no hay lugar a duda por cuanto respecta al reconocimiento de los derechos de consulta, registro, rectificación y cancelación de datos, reconocidos en el reseñado artículo y siguientes de la *Ley Orgánica 15/1999*, no es tampoco discutible que se ha de proporcionar al ciudadano el derecho a ser borrado para siempre del entorno cibernético[22].

Dato normativo: especial referencia a la LOPD, Directiva 95/46 y Reglamento de Protección de Datos de la Unión Europea

La norma europea que marcó la línea a seguir en materia de protección de datos fue el *Convenio nº 108 del Consejo de Europa*[23], más conocido como *Convenio para la protección de las personas en lo relativo al tratamiento automatizado de datos de carácter personal*, que entró en vigor el 1 de octubre de 1985. El Convenio pretendía garantizar a cualquier persona física, con independencia de su nacionalidad o residencia, el respeto de sus derechos y libertades fundamentales, concretamente el derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a la persona. El Convenio recoge en el capítulo segundo unos principios básicos para la protección de datos, entre los que destaca el principio del derecho al olvido.

Posteriormente, fue aprobada en el ámbito comunitario la *Directiva 95/46/CE*[24]*, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales*[25] *y a la libre circulación de estos datos*; constituye el texto de referencia, a escala europea, en materia de protección de datos personales. Crea un marco regulador destinado a establecer un equilibrio entre un nivel elevado de protección de la vida privada de las personas y la libre circulación de datos personales dentro de la Unión Europea, o dicho de otro modo, sienta las bases para conseguir que no existan diferencias entre los niveles de protección de los derechos y libertades de las personas y, en particular, de la intimidad, garantizados en los Estados miembros en lo que se refiere al tratamiento de datos personales. Con ese objeto, la Directiva fija límites estrictos para la recogida y utilización de los datos personales y solicita la creación, en cada Estado miembro, de un organismo nacional independiente encargado de la protección de los mencionados datos[26].

Hay que hacer referencia, por último, a legislación española en esta materia.

El desarrollo legislativo se lleva a cabo mediante la *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal*[27], que supuso la transposición de la Directiva 95/46/CE a nuestro ordenamiento interno. El objetivo de la LOPD es garantizar y proteger las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar, en lo que concierne al tratamiento de datos personales.

Como cabe deducir de lo anteriormente expuesto, contamos con normativa sobre la materia, pero hemos de ser conscientes de que con los avances tecnológicos que surgen se hace necesario modernizar cada cierto tiempo el marco jurídico en relación a la protección de datos.

Si bien es cierto, en todas las normas citadas hasta el momento no se recoge expresamente un "derecho al olvido" como tal, aunque como se ha venido apuntando podría deducirse de una interpretación extensiva del derecho de cancelación (contemplado en los art. 16 de la LOPD y 12 de la Directiva 95/46) coherente y conforme a las nuevas tecnologías y herramientas de Internet. No obstante, la situación puede cambiar, merced al reconocimiento social que empieza a darse del mencionado derecho y la repercusión de la citada referencia jurisprudencial cuyo impacto podemos afirmar que ha sido a nivel mundial, encontrando ya a nivel nacional la primera sentencia civil que se pronuncia respecto al controvertido derecho al olvido, sentencia emitida por la Audiencia Provincial de Barcelona (Sección 16ª, de fecha 17 de julio de 2014, resolviendo un recurso de apelación formulado contra la sentencia del Juzgado de Primera Instancia nº 8 de Barcelona) que siguiendo la misma línea del TJUE, determina que existe responsabilidad de Google por vulnerar el derecho a la protección de datos.

En este sentido, hemos de poner de manifiesto que el Borrador de *Reglamento de Protección de Datos de la Unión Europea*[28] contemplaba ya como derecho de los titulares de datos el "derecho a ser olvidados", entendiendo por tal que los datos que un día fueron facilitados sean ahora cancelados a petición de los interesados cuando ya no son necesarios o el periodo de almacenaje ya ha expirado. Los antecedentes informáticos dejarían de estar accesibles en la Web y no serían localizables tampoco a través de los buscadores genéricos.

En este sentido, según señala Pere Simón, la AEPD viene trabajando sobre el tema de un modo similar a como han venido defendiendo la *Commission Nationale de l´Infromatique et les Libertés* (CNIL), en Francia, y el *Garante per la Protezioni dei Dati Personali*, en Italia, y reconoce la existencia del derecho al olvido digital relacionándolo fundamentalmente con el derecho a la protección de datos.

El *borrador,* tal como se planteaba de forma inicial, desarrollaba los derechos de los interesados a partir del capítulo III (art. 9 y ss.), interesando poner de relieve que es a partir de la sección tercera (art.14 y ss.) cuando comienza a tratar la rectificación y la cancelación, ocupándose primeramente del derecho de

rectificación (art.14) y de forma detallada contemplando el derecho a ser olvidado y borrado en su artículo 15.

Finalmente en el art. 17 de su actual redacción, se da cabida de forma literal al derecho al olvido y a la supresión, encontrando dentro del extenso contenido del artículo una mención expresa a que el interesado podría suprimir todos aquellos datos que no fueran necesarios, y de igual modo podría pedir su retirada cuando el periodo de almacenamiento consentido hubiera expirado.

Se pretende además dar con la solución idónea para eliminar de forma permanente aquellos datos puestos a disposición de los distintos servicios informáticos cuando el usuario sea menor de edad. Por último señalar que también hace alusión a que el borrado incluirá la eliminación de todos los enlaces de Internet que contuvieren la información que se desea suprimir y contempla como se pondrán en práctica los mecanismos oportunos para asegurar que se cumplan los plazos establecidos para eliminar la información que el interesado ha solicitado que sea cancelada.

La necesidad del reconocimiento efectivo de un derecho de supresión, lo que se ha venido denominando con anterioridad a que el Parlamento Europeo diera luz verde al proyecto de reforma del Reglamento Europeo de Protección de Datos, derecho al olvido, se puede incluso fundamentar constitucionalmente a través del art. 18.4, que hace mención expresa a que la ley tiene que limitar el uso de la informática en aras de salvaguardar el honor y la intimidad de las personas.

Por situarnos en el tiempo, señalar que el 21 de octubre de 2013, la Comisión de Libertades Civiles, Justicia y Asuntos de Interior del Parlamento Europeo (LIBE) emitió un informe definiendo su posición con respecto al borrador de Reglamento General de Protección de Datos. La Comisión LIBE planteó llevar a cabo algunas modificaciones con respecto al borrador original del que hemos venido hablando en las líneas precedentes (Reglamento presentado por la Comisión Europea en enero de 2012), entre ellas, por cuanto interesa para este artículo, destacar el ya mencionado cambio de tratamiento que se da al "derecho al olvido" que pasa a llamarse "derecho de supresión", no variando, en líneas generales, su regulación.

El 12 de marzo de 2014, el Parlamento Europeo da luz verde al proyecto de reforma del Reglamento Europeo de Protección de Datos, a falta solo del visto bueno del Consejo para su aprobación definitiva.

Simplemente a efectos de informar al lector sobre dónde radica la importancia de la aprobación del Reglamento por cuanto a repercusión práctica se refiere, destacar que se trata de una adaptación de la protección de datos a las nuevas prácticas del mundo digital, evitando en la medida de lo posible las divergencias en la aplicabilidad de las normas por parte de los distintos Estados miembros al tiempo que se vela por la efectiva aplicación de los derechos fundamentales implicados en el uso de las nuevas tecnologías. Así mismo se trata de aumentar la

confianza del consumidor mediante la introducción del derecho a la rectificación, al olvido y a la supresión, así como el derecho a la portabilidad de datos y de oposición.

Ponderación de derechos: libertad de expresión, intimidad y protección de datos

Un problema no ajeno a la consideración de estas cuestiones es el que pone de relieve que en un entorno tan específico como es el de Internet, con el flujo tan importante de información que circula en la Red, y teniendo en cuenta los avances informáticos, no parece complicado poder comprometer alguno de los derechos constitucionalmente reconocidos como derechos de la persona. Por un lado el derecho a expresarse libremente: Internet pone a nuestra disposición el entorno perfecto para hacer efectivo este derecho, sin embargo no es complicado que el ejercicio de tal derecho comprometa en modo alguno derechos como la intimidad o la protección de datos. A través del respeto se debe procurar la convivencia pacífica de todos ellos.

No es cuestión baladí el pretender apuntar, por lo tanto, que el uso masivo de las nuevas tecnologías crea un marco peligroso para la intimidad.

La incesante inclusión por los propios usuarios de datos en la Red está acarreando situaciones en las que determinados derechos básicos de la persona se están viendo incesantemente vulnerados, en concreto la intimidad, considerada por la doctrina como un derecho de la personalidad, subjetivo y de defensa[29], aunque no de forma exclusiva, pues en ocasiones se pueden ver afectados otros derechos interrelacionados como el derecho al honor o a la propia imagen.

Ponderar los intereses en conflicto para poder determinar cuál de ellos debe prevalecer es una cuestión cuya solución va a depender de las circunstancias de cada caso y del tipo de información que se vea comprometida, así como el carácter que esta tenga respecto a calificarla o no como información pública o fuente de acceso público[30], término que resulta igualmente problemático.

El concepto jurídico de intimidad encuentra su origen en un artículo de Warren y Brandeis[31], en el que se viene a concluir que su reconocimiento se hace necesario para poder proteger a las personas frente posibles intrusiones ajenas, excluyendo, por lo tanto, toda comunicación, publicación o intervención que cualquier tercero pudiese hacer respecto a datos de nuestra vida. Recogido en el ya citado artículo 18.1 de la CE, el derecho a la intimidad está considerado como uno de los derechos de la persona más importantes dentro de nuestro ordenamiento jurídico.

Poniendo lo anteriormente dicho en conexión directa con el tema tratado, conviene redundar en que la finalidad principal del derecho al olvido o supresión

no es otra que preservar el ámbito de la privacidad de todos los individuos y que su regularización se encamina a conceder un ámbito mayor a la intimidad, a través de las facultades de cancelación y oposición al tratamiento de ciertos datos de carácter personal vinculados a experiencias del pasado que pueden comprometer nuestra imagen o nuestra vida en sentido amplio en el futuro.

La jurisprudencia del Tribunal Constitucional se ha pronunciado en multitud de sentencias y tiende a dar preferencia a la libertad de expresión frente a otros derechos constitucionales tales como el derecho al honor o a la intimidad, eso sí, siempre que los hechos comunicados en los distintos medios se consideren de relevancia pública (Sentencias del Tribunal Constitucional 105/1983 y 107/1988) y atendiendo a la veracidad de la información publicada (Sentencias del Tribunal Constitucional 6/1988, 105/1990 y 240/1992). A *sensu contrario*, la intimidad prevalece en los casos en los que se trata de hechos o personas no públicas, o cuando la información no es veraz.

Siguiendo esta misma línea, varias de las resoluciones[32] de la AEPD han considerado que, aunque se puedan encontrar informaciones publicadas que han sido contrastadas y cuya veracidad se reconozca, al no referirse a asuntos de relevancia pública y, por tanto, de interés general, debe prevalecer el derecho fundamental de protección de datos frente a la libertad de expresión e información.

En este punto es conveniente rescatar la Sentencia de la Audiencia Nacional del 10 de noviembre de 2006, que hace una valoración de la libertad de la información veraz como a continuación se expone:

> *« […] ninguna objeción puede hacerse a la finalidad que persigue el derecho a la libertad de información veraz, pero dicho derecho fundamental no es un derecho absoluto, sino que hay que ponerlo en relación con otros derechos fundamentales, como lo es en este caso, el derecho fundamental a la protección de datos al que se refiere la STC 292/2000, de 30 de noviembre de 2000».*

Por todo lo expuesto, la AEPD ha interpretado[33] que ningún ciudadano que no goce de la condición de personaje público ni sea considerado persona de relevancia pública por algún hecho sucedido, tiene que soportar que sus datos de carácter personal circulen por la Red, sin poder poner los medios necesarios para corregir la inclusión ilegítima de sus datos en un sistema de comunicación universal como es Internet. Así mismo, en el criterio establecido por esta institución, se reconoce que el ciudadano que no esté obligado a someterse a la disciplina del ejercicio de las libertades de expresión e información debe gozar de mecanismos reactivos amparados en Derecho que impidan el mantenimiento secular y universal en la Red de su información de carácter personal.

Destacar por último, en relación con la responsabilidad de los proveedores de búsquedas y enlaces, la Sentencia de la Audiencia Provincial de Madrid de 19 de Febrero de 2010 ante la pretensión de un afectado por el caso Malaya de que se salvaguardase su honor impidiendo que Google indicase un enlace de la

web de Telecinco y de otro programa de tertulianos, se le desestimó su demanda y se le contestó que el art. 17 de la *Ley 34/2002, de 11 de junio, de Servicios a la Sociedad de la Información y de Comercio Electrónico,* exime a Google, como prestador de servicios de intermediación, de toda responsabilidad por la información que dirija a sus destinatarios, siendo lo adecuado demandar en su caso a Telecinco o al programa responsable de la página enlazada.

En resumen, todo parece apuntar a una clara ponderación del derecho a la intimidad a través de la protección de datos en contraposición a los derechos de información y de libertad de expresión, salvo, como se extrae de la jurisprudencia anteriormente señalada, en aquellos casos en que se trate de información de carácter público o de individuos que ostenten la condición de personajes públicos.

Conclusiones

En esta Sociedad del Conocimiento, los usuarios de Internet parecen no tener ningún derecho a controlar los datos que sobre sí mismos circulan en la Red y precisamente eso es lo que hay que empezar a controlar. El reconocimiento efectivo de un derecho al olvido digital, o un derecho de supresión como se ha pasado a llamar, operaría en la práctica como una herramienta más, complementaria a los mecanismos existentes que caminan en la mima línea, es decir, los contemplados en el art. 16 de la LOPD relativos a la rectificación o la cancelación; su reconocimiento contribuiría de forma incuestionable a la consecución del fin que se pretende: desaparecer de la Red.

A estas alturas no cabe duda de que el ciberespacio proporciona todo tipo de información, y permite estar en conexión permanente con el resto del mundo, pero lamentablemente hay fallos y uno de los más graves es que en la actualidad no se garantiza el poder borrar los datos que el usuario quiere que desaparezcan de forma permanente del entorno virtual, provocando en los internautas un alto grado de inseguridad ante la posibilidad de que el pasado pueda comprometer el futuro.

Hace algún tiempo parecía que los obstáculos para poder suprimir cierta información solo hacían que multiplicarse en lugar de disminuir y los mecanismos existentes no parecían dar respuesta o ser lo suficientemente efectivos para lograr que determinada información que circulaba por la Red cayese en el olvido. La AEPD ha venido y viene trabajando sobre el tema; muestra de ello es la Sentencia del TJUE, cuyo reconocimiento al derecho al olvido queda amparado por el art. 18.4 de la Constitución Española.

Parece, por tanto, que los esfuerzos encaminados a que los motores de búsqueda no indexen determinados datos personales a petición de los usuarios, finalmente, se han visto recompensados. Solo falta que el *Reglamento de Protección*

de Datos de la UE se apruebe y con ello se reconozca el ahora llamado derecho de supresión que no es otra cosa que el derecho a ser olvidado o borrado de la memoria de Internet, y en definitiva viene a ser una aplicación del ya reconocidísimo derecho de cancelación, contemplado en el reseñado art. 16 de la LOPD, pero orientado ahora al ámbito de Internet.

Con este horizonte a la vista no es extraño que contemos no solo con el primer pronunciamiento a nivel europeo, sino con la primera sentencia española de la Audiencia Provincial de Barcelona, que no hace sino que caminar en la misma línea que la emitida por la Corte con Sede en Luxemburgo y que ha sentado un precedente para regular las relaciones entre los usuarios y las compañías que operan en la Red.

Pese a que la jurisprudencia sigue hablando de "derecho al olvido" no hay que olvidar que en la actualidad se ha pasado a denominar derecho de supresión, y que no es más que aquel derecho mediante el cual cualquier persona podría solicitar que se borren sus datos, operando en la praxis si se dan cualquiera de las circunstancias que a continuación se relacionan: si no se cumplen las normas de la UE, si los datos ya no son necesarios, o si la persona retira o no da su consentimiento al almacenamiento de esa información. Es en esencia lo mismo que venía a dar forma al derecho al olvido.

En conclusión, a nuestro modo de ver, es cuestión urgente que se apruebe definitivamente el Reglamento, independientemente de cómo se denomine el *derecho controvertido* bien sea derecho al olvido o derecho de supresión, puesto que, además de lo que esto supondría cara a la protección de la intimidad, se estaría logrando la armonización de la regulación relativa a la protección de datos.

Si bien es cierto todo lo anteriormente expuesto, como última reflexión para cerrar el artículo, merece la pena destacar que es fundamental ser conscientes del hecho de que las políticas de los sitios webs sobre el tratamiento de datos a veces olvidan el deber jurídico de informar como pilar fundamental del consentimiento válidamente otorgado, lo que hace que el usuario se vea perjudicado ante tal circunstancia; por eso es importante que, antes de tener que usar el remedio que supondría ejercitar el derecho a ser olvidado, se abogue por un mayor conocimiento y arraigo de una cultura de protección de datos.

Bibliografía

CABALLERO GEA, J.A. (2007). *Derecho al honor, a la intimidad personal y familiar y a la propia imagen. Derecho de Rectificación. Calumnia e Injuria*, Dykinson.

CARRILLO LÓPEZ, M. (2003). *El derecho a no ser molestado*, Tecnos.

CASTILLO JIMÉNEZ, C. (2001). *Protección del derecho a la intimidad y uso de las nuevas tecnologías de la información*, Derecho y Conocimiento, Huelva.

DAVARA RODRÍGUEZ, M.A. (2007). *Código de Internet*, Aranzadi.
DAVARA RODRÍGUEZ, M.A. (2003). *Manual de Derecho Informático*, Aranzadi.
GÓMEZ MARTÍNEZ C. (2004). *Derecho a la intimidad y nuevas tecnologías*, Cuadernos de Derecho Judicial.
LUCAS MURILLO DE LA CUEVA, P. (1990). *El derecho a la autodeterminación informativa*, Tecnos.
MARTÍNEZ MARTÍNEZ, R. (2004). *Una aproximación crítica a la autodeterminación informativa*, Civitas.
MESSÍA DE LA CERDA BALLESTEROS, J.A. (2003) *La Cesión o Comunicación de datos de Carácter Personal*, Thomson, Civitas.
REBOLLO DELGADO, L. (2005) *El derecho fundamental a la intimidad*, Dykinson.
SÁNCHEZ, A., SILVERA, H., Y NAVARRO, M. (2003). *Tecnología, intimidad y sociedad democrática*, Icaria.

Notas

[1] Abogada. Doctoranda en Derecho Civil en la Universidad de Salamanca. Miembro del Proyecto I+D+i del Ministerio de Economía y Competitividad (Programa Estatal de Investigación, Desarrollo e Innovación Orientada a los Retos de la Sociedad), "Privacidad y Redes Sociales: Nuevos retos en la protección de datos y de los derechos al honor, intimidad e imagen" (DER2013-42294-R).

[2] Conjunto de aplicaciones y páginas de Internet que proporcionan al usuario el control de sus datos, y la edición de contenidos, permitiéndole pasar de ser exclusivamente consumidor a convertirse en un productor y creador.

[3] Messía de la Cerda Ballesteros, J.A., *La cesión o comunicación de datos de carácter personal*, Cap. I, pág. 27 y ss., Civitas, 2003. Capítulo I, pág. 27 y ss.

[4] El disponer de un dato tan aparentemente insignificante como el correo electrónico de una persona puede permitir el llegar a conocer su identidad de forma precisa, pues aunque no sea una dirección elaborada a partir de datos propios como el nombre o apellidos, que suele ser algo común en la práctica, podemos llegar de forma exacta e inequívoca de quién se trata a través de su dirección IP, por este motivo, actualmente se considera dentro de la identificación de dato de carácter personal la IP o los datos de localización.

[5] http://www.agpd.es/portalwebAGPD/canaldocumentacion/textos_interes/common/pdfs/aepd_dpa_es.pdf [último acceso el 16 de septiembre de 2014].

[6] http://tecnologia.elpais.com/tecnologia/2011/12/25/actualidad/1324807261_850215.html (último acceso el 21 de septiembre de 2014).

[7] http://www.abc.es/20120216/tecnologia/rww-abci-aplicacion-para-moviles-twitter-201202161057.html [último acceso el 21 de septiembre de 2014].

[8] http://alt1040.com/2012/01/los-problemas-de-seguridad-de-whatsapp-y-3-alternativas [último acceso el 21 de septiembre de 2014].
http://www.trecebits.com/2012/03/07/los-problemas-de-seguridad-de-whatsapp-son-casi-imposibles-de-arreglar/ [último acceso el 21 de septiembre de 2014].

[9] http://www.abc.es/tecnologia/moviles-aplicaciones/20140825/abci-whastsapp-numero-usuarios-line-tango-viber-201408250904.html [último acceso el 25 de noviembre de 2014].

[10]http://www.genbeta.com/mensajeria-instantanea/whatsapp-da-un-salto-enorme-en-seguridad-integrando-cifrado-de-punto-a-punto [último acceso el 26 de noviembre de 2014].

[11]Memoria anual 2009 de la AEPD.

[12] Según datos extraídos de: http://www.softandapps.info/2011/08/27/10-de-las-principales-redes-sociales-en-numeros-infografia/ [último acceso el 21 de septiembre de 2014].

[13] Tuenti es una red social enfocada a la población española, a la cual solo se podía acceder por invitación, hasta el 14 de noviembre de 2011. Funciona como cualquier otra red social permitiendo al usuario crear su propio perfil, añadir a otros usuarios como amigos e intercambiar mensajes, crear eventos, subir fotos y videos.

[14] El problema se puede trasladar también al caso ya apuntado de los menores; en multitud de ocasiones, publican contenidos desconociendo la incidencia de divulgar ciertas informaciones o "colgar" ciertas fotos o subir determinados vídeos, que no solo pueden comprometer a su persona sino también a terceros por contener imágenes potencialmente perjudiciales para su integridad, o informaciones potencialmente humillantes.

[15] Es un programa o un pequeño fragmento de software que incrementa o aumenta las funcionalidades de un programa principal.

[16] El GT29 fue creado por la Directiva 95/46/CE. Tiene carácter de órgano consultivo independiente y está integrado por las Autoridades de Protección de Datos de todos los Estados miembros. La Agencia Española de Protección de Datos forma parte del mismo desde su inicio, en febrero de 1997.

[17] Estas y otras cuestiones son tratadas por el GT29 en el *Dictamen sobre cuestiones de protección de datos en relación con los buscadores*, de fecha 4 de abril de 2008.

[18] Disponible a través del siguiente enlace: http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=ES [último acceso el 25 de noviembre de 2014].

Como cuestiones importantes extraídas de la propia sentencia destacar que la misma establece:

- La actividad de los motores de búsqueda como Google constituye un tratamientode datos de carácter personal, del que es responsable el propio motor, dado que este determina los fines y los medios de esta actividad.
- Ese tratamiento está sometido a las normas de protección de datos de la UE, dado que Google ha creado en un Estado miembro un establecimiento para la promoción y venta de espacios publicitariosy cuya actividad se dirige a los habitantes de ese Estado.
- Las personas tienen derecho a solicitar del motor de búsqueda, con las condiciones establecidas en la Directiva de protección de datos, la eliminación de referencias que les afectan, aunque esta información no haya sido eliminada por el editor ni dicho editor haya solicitado su desindexación. En caso de no atenderse su solicitud, las personas tienen derecho a recabar la tutela de la AEPD y de los Tribunales.
- El derecho a la protección de datos de las personas prevalece, con carácter general, sobre el "mero interés económico del gestor del motor de búsqueda" salvo que el interesado tenga relevancia pública y el acceso a la información esté justificado por el interés público.

[19] No hay que perder de vista que en la práctica esto puede acarrear consecuencias negativas si se usa el fallo de forma fraudulenta con el fin de lograr que desaparezca de Internet información de competidores, por lo que se hace necesario en todo caso verificar la identidad del solicitante.

[20] Rallo Lombarte, A., *Cuadernos de Comunicación e Innovación Telos* Nº85, octubre-diciembre de 2010.

[21] Palabras que ponen de relieve que los buscadores genéricos son meros intermediarios, no pudiendo por tanto considerarlos responsables de los contenidos informativos a los que facilitan el acceso. La relevancia de esta idea es clara en orden a su responsabilidad a la luz de lo establecido en el artículo 16 de la Ley de Servicios de la Sociedad de la Información (LSSI) aunque tal desarrollo excede del marco del presente trabajo.

[22] Lo que Ramón Rey Ruíz denomina obligación de una "amnesia digital", Vid. El artículo publicado en *Legaltoday.com* de fecha 15 de octubre de 2014, accesible a través del siguiente enlace: http://www.legaltoday.com/practica-juridica/publico/proteccion_de_datos/la-amnesia-digital-y-el-derecho-al-olvido-cara-y-cruz-de-la-misma-moneda [último acceso el 26 de noviembre de 2014].

[23] Convenio nº 108 del Consejo de Europa, de 28 de enero de 1981. Disponible a través del siguiente enlace: http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm [último acceso 21octubre de 2014].

[24] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la *protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de datos*. (complementada por la Directiva 97/66/CE, hoy sustituida por la 2002/58/CE).

[25] Pudiendo apoyarse en lo dispuesto en el artículo 8.2 de la *Carta de Derechos fundamentales de la Unión Europea*.

[26] http://europa.eu/legislation_summaries/information_society/data_protection/l14012_es.htm [último acceso 21 de septiembre de 2014].

[27] Supuso la derogación de la *Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal,* conocida como la LORTAD (vigente hasta el 14 de enero de 2000).

[28] http://statewatch.org/news/2011/dec/eu-com-draft-dp-reg-inter-service-consultation.pdf [último acceso octubre de 2014].

[29] Esta votación posiciona al Parlamento de cara a las negociaciones con el Consejo y la Comisión Europea (fase que se conoce como "diálogo a tres bandas"). El objetivo de la Comisión LIBE es que su informe se votara de forma plenaria en el Parlamento Europeo en el mes de marzo, anticipándose a las elecciones al Parlamento. Según se desprende de la información obtenida a través del siguiente enlace: http://www.apep.es/la-comisin-libe-de-la-ue-aprueba-el-reglamento-de-proteccin-de-datos/ [último acceso el 26 de noviembre de 2014].

[30] Carrillo López, M., *El derecho a no ser molestado*, Tecnos, 2003; Lucas Murillo de la Cueva, P., *El derecho a la autodeterminación informativa*, Tecnos, 1990; Rebollo Delgado, L., *El derecho fundamental a la intimidad*, Dykinson, 2005; Lucas Murillo de la Cueva, P., *El derecho a la autodeterminación informativa*, Tecnos, 1990.

[31] Hay que ponderar el derecho a la privacidad del usuario frente al derecho público a conocer y distribuir información.

[32] Warren and Brandeis, *The Right to Privacy*, Harvard Law Review, Vol. IV, Diciembre, 1890 No. 5.

[33] P. ej.: Resolución nº.: R/00598/2007; Resolución nº.: R/00347/2011; Resolución nº.: R/01258/2010; Resolución nº.: R/01942/2010.

[34] Al respecto consúltense las Resoluciones citadas en la nota precedente.